METHOD AND APPARATUS FOR FACILITATING USE OF A PRE-SHARED SECRET KEY WITH IDENTITY HIDING

ABSTRACT

One embodiment of the present invention provides a system that facilitates a key exchange that operates with a pre-shared secret key and that hides identities of parties involved in the key exchange. The method operates by establishing a negotiated secret key between a first party and a second party by performing communications between the first party and the second party across a network in a manner that does not allow an eavesdropper to determine the negotiated secret key. Next, the system encrypts an identifier for the first party using the negotiated secret key and a group secret key to form an encrypted identifier. This group secret key is known to members of a group, including the first party and the second party, but is kept secret from parties outside of the group. Next, the system sends the encrypted identifier from the first party across the network to the second party. This allows the second party to decrypt the encrypted identifier by using the negotiated secret key and the group secret key, so that the second party can use the identifier to lookup the pre-shared secret key that was previously established between the first party and the second party. This pre-shared secret key is subsequently used in forming at least one subsequent communication between the first party and the second party.